United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Thursday,
May 18, 2000

CRITICAL INFRASTRUCTURE PROTECTION

"ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

20000519 029

G A O
Accountability * Integrity * Reliability

GAO/T-AIMD-00-181

DTIC QUALITY INSPECTED 2

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the "ILOVEYOU" computer virus. Accompanying me today is Keith Rhodes, Director of GAO's Office of Computer and Technology Assessment. As you know, ILOVEYOU is the latest in a series of Internet-based episodes that have caused serious disruptions to computer-based operations at both private businesses and government agencies. While the federal government is working to implement mechanisms that would help agencies to ward off such an attack, it was not effective at detecting this virus early on and warning agencies about the imminent threat. Consequently, most agencies were affected. Some incurred damage to systems and files and many others spent countless staff hours fending off the attack and reestablishing e-mail service. Overall, however, once they learned of the virus, agencies responded promptly and appropriately.

In addition to discussing the virus, I would like to address its impact on federal agencies as well as measures that can be taken to mitigate the effects of future attacks, which promise to be increasingly sophisticated and damaging and harder to detect.

The ILOVEYOU Worm/Virus

ILOVEYOU is both a "virus" and "worm." Worms propagate themselves through networks; viruses destroy files and replicate themselves by manipulating files. The damage resulting from this particular hybrid—which includes overwhelmed e-mail systems and lost files–is limited to users of the Microsoft Windows operating system.

ILOVEYOU typically comes in the form of an e-mail message from someone the recipient knows with an attachment called LOVE-LETTER-FOR-YOU.TXT.VBS. The attachment is a Visual Basic Script (VBS) file.[1] As long as recipients do not run the attached file, their systems will not be affected and they need only to delete the e-mail and its attachment. When opened and allowed to run, however, ILOVEYOU attempts to send copies of itself using Microsoft Outlook (an electronic mail software program) to all entries in all of the recipient's address books. It attempts to infect the Internet Relay Chat (IRC) program[2] so that the next time a user starts

[1]VBS is a subset of Microsoft's Visual Basic program language intended for use in World Wide Web browsers and certain other applications.

[2]A program that enables people connected anywhere on the Internet to join in live discussions. Unlike older chat systems, IRC is not limited to just two participants. The IRC client sends the participant's messages to and receives messages from an IRC server. The IRC server is responsible for making sure that all messages are broadcast to everyone participating in a discussion.

"chatting" on the Internet, the worm can spread to everyone who connects to the chat server. It searches for picture, video, and music files and attempts to overwrite or replace them with a copy of itself. In addition, the worm/virus further attempts to install a password-stealing program that would become active when the recipient opened Internet Explorer[3] and rebooted the computer. However, Internet accounts set up to collect to stolen passwords were reportedly disabled early in the attack.

The worm/viruses also appeared in different guises–labeled as "Mother's Day," "Joke," "Very Funny," among others. These variants retriggered disruptions because they allowed the worm/virus to bypass filters set up earlier to block ILOVEYOU. At least 14 different versions of the virus have been identified, according to the Department of Defense's (DOD) Joint Task Force-Computer Network Defense. One, with the subject header "VIRUS ALERT!!!", was reportedly even more dangerous than the original because it was also able to overwrite system files critical to computing functions.

The difference between ILOVEYOU and other recent viruses, such as the Melissa virus, which surfaced about this time last year, is the speed at which it spread. Soon after initial reports of the worm/virus surfaced in Asia on May 4, ILOVEYOU proliferated rapidly throughout the rest of the world. By 6 p.m. the same day, Carnegie Mellon's CERT Coordination Center (CERT-CC)[4] had received over 400 direct reports involving more than 420,000 Internet hosts. One reason ILOVEYOU multiplied much faster than Melissa was that it came during the work week, not the weekend. Moreover, ILOVEYOU sent itself to everyone on the recipient's e-mail lists, rather than just the first 50 addressees as Melissa did. The following two figures provide a more detailed overview of the timelines associated with the introduction of the virus and the subsequent discovery and notification actions taken by various entities.

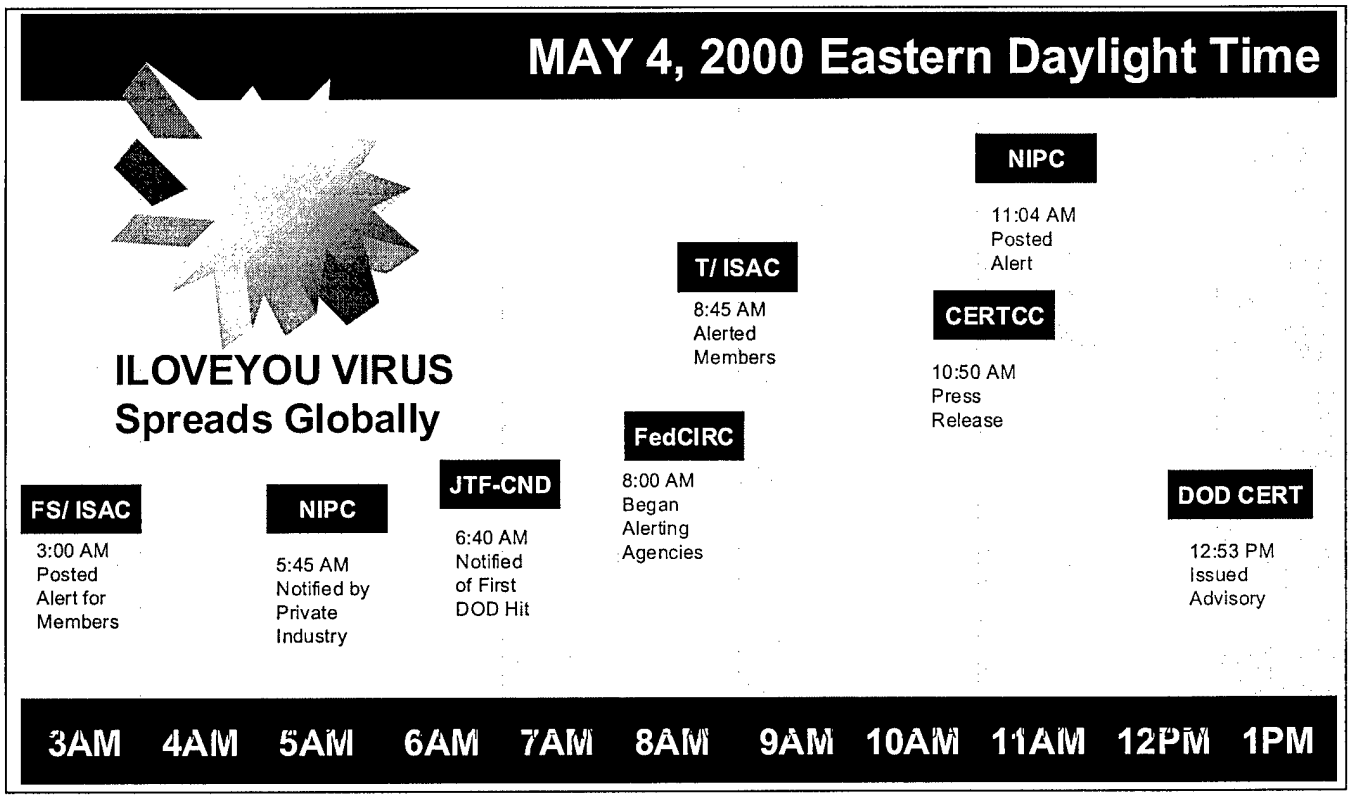
[3]Microsoft's World Wide Web browser.

[4]Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with and respond to incidents and to build awareness of security issues across the Internet community.

Figure 1: Highlights of Events Relating to the ILOVEYOU Virus

- The virus began proliferating during business hours in the Far East, while the United States—a 12-hour time difference away—was still sleeping. The virus spread with unprecedented speed through Asia and Europe. By the time it was 3 p.m. in Hong Kong, it was 9 a.m. in Western Europe and the impact of the virus was becoming evident.
- Meanwhile, a private sector group, the Financial Services Information Sharing and Analysis Center (FS/ ISAC), had also discovered the virus and, at approximately 3 a.m. EDT, posted an alert to its members.
- At 5:45 a.m. EDT, a representative from private industry notified the National Infrastructure Protection Center (NIPC), located at the Federal Bureau of Investigation, of the problem.
- The Department of Defense Joint Task Force for Computer Network Defense (JTF-CND), which operates a 24-hour global operation center, was first alerted that the virus had hit DOD at 6:40 a.m. EDT by one of the military services. After about an hour of analysis to determine the nature of the virus, JTF-CND began to notify the various DOD components individually.
- By 7:18 a.m. EDT, the Telecommunications Information Sharing and Analysis Center (T/ISAC) received a message that one of its major carriers was "taking severe actions to close its e-mail gateways" because of the ILOVEYOU virus.
- At 7:45 a.m. EDT—2 hours after it was first notified of the virus—the NIPC notified FedCIRC of the rapidly spreading virus, and FedCIRC began notifying senior agency officials via phone and fax.
- At 11:00 a.m. EDT, the NIPC posted a short alert paragraph on its home page warning about the ILOVEYOU virus. At about the same time, the CERT-CC sent an e-mail to the media stating that it had received over 150 reports of the virus.

Figure 2: Illustrated Timeline



In addition to hitting most federal agencies—discussed later in my statement—the worm/virus affected large corporations, such as AT&T, TWA, and Ford Motor Company; media outlets, such as the Washington Post, Dow Jones, and ABC news; state governments; school systems; and credit unions, among many others, forcing them to take their networks off-line for hours. Internationally, the virus affected businesses, organizations, and governments, including the International Monetary Fund, the British Parliament, Belgium's banking system, and companies in the Baltics, Denmark, Italy, Germany, Norway, the Netherlands, Sweden, and Switzerland.

The bottom line in terms of damage is still uncertain. Initial estimates of damage from the outbreak ranged from $100 million to over $10 billion

globally. We do not have a basis for commenting on overall loss. While press reports are full of anecdotal accounts from disparate sectors of the economy, it is difficult to reliably and precisely estimate factors such as loss of productivity, lost opportunity costs, reductions in customer confidence, slow down of technical staff, and loss of information. Furthermore, as with most security incidents, companies affected are not likely to fully disclose the true extent of their losses.

Despite Efforts to Enhance Federal Response to Computer Attacks, Agencies Were Not Effectively Warned About ILOVEYOU

Recognizing the increasing computer-based risks to our nation's critical infrastructures, the federal government has taken steps over the past several years to create capabilities for effectively detecting, analyzing, and responding to cyber-based attacks. However, the events and responses spawned by ILOVEYOU demonstrate both the challenge of providing timely warnings against information-based threats and the increasing need for the development of national warning capabilities.

The National Infrastructure Protection Center (NIPC), located in the Federal Bureau of Investigation, is responsible for serving as the focal point in the federal government for gathering information on threats as well as facilitating and coordinating the federal government's response to incidents affecting key infrastructures. Presidential Decision Directive 63 (PDD 63) which was signed in May 1998, also specifically charged the NIPC with issuing attack warnings as well as alerts to increases in threat condition. This includes warnings to private sector entities.

Developing the capability to provide early warning of imminent cyber-based threats is complex and challenging but absolutely essential to the assigned NIPC mission. Data on possible threats—ranging from viruses, to hoaxes, to random threats, to news events, and computer intrusions—must be continually collected and analyzed from a wide spectrum of globally distributed sources. Moreover, once an imminent threat is identified, appropriate warnings and response actions must be effectively coordinated among federal agencies, the private sector, state and local governments, and even other nations. It is important that this function be carried out as effectively, efficiently, and quickly as possible in order to ensure continuity of operations as well as minimize disruptions.

To date, the NIPC has had some success in providing early warning about impending threats. For example, in December 1999, it posted warnings about a rash of denial-of-service attacks prominently on its website and it offered a tool that could be downloaded to scan for the presence of the denial-of-service code. Two months later, the attack arrived in full force, compromising the services of Yahoo, E-Bay, and other Internet companies.

However, the NIPC had less success with the ILOVEYOU virus. As noted earlier (in figure 1), the NIPC first learned of the virus at 5:45 a.m. EDT from an industry source. Over the next 2 hours, the NIPC checked other sources in attempts to verify the initial information with limited success. According to NIPC officials, no information had been produced by intelligence, Defense, and law enforcement sources, and only one reference was located in open sources, such as Internet websites. The NIPC considers assessment of virus reports to be an important step before issuing an alert because most viruses turn out to be relatively harmless or are detected and defeated by existing antivirus software. According to the NIPC, the commercial antivirus community identifies about 20 to 30 new viruses every day, and more than 53,000 named viruses have been identified to date. At 7:40 a.m., two DOD sources notified the NIPC that the virus was spreading through the department's computer systems, and the NIPC immediately notified the Federal Computer Incident Response Center (FedCIRC), at GSA, and CERT-CC. FedCIRC then undertook a rigorous effort to notify agency officials via fax and phone.

For many agencies, this was too late. In fact, only 2 of the 20 agencies we spoke with reported that they first learned of the virus from FedCIRC. Twelve first found out from their own users, three from vendors, two from news reports, and one from colleagues in Europe. NIPC did not issue an alert about ILOVEYOU on its own web page until 11 a.m., May 4—hours after many federal agencies were reportedly hit. This notice was a brief advisory; the NIPC website did not offer advice on dealing with the virus until 10 p.m. that evening.

For the most part, agencies themselves responded promptly and appropriately once they learned about the virus. In some cases, however, getting the word out was difficult. At DOD, for example, the lack of teleconferencing capability slowed the JTF-CND response because Defense components had to be called individually. At the Department of Commerce, cleanup and containment efforts were delayed because many of the technical support staff had not yet arrived at work when users began reporting the virus. The National Aeronautics and Space Administration (NASA) also had difficulty communicating warnings when e-mail services disappeared. And while backup communication mechanisms are in place, NASA officials told us that they are rarely tested. Justice officials similarly learned that the department needed better alternative methods for communicating when e-mail systems are down. Additionally, many agencies initially tried to filter out reception of the malicious "ILOVEYOU" messages. However, in doing so, some also filtered out e-mail alerts and communications regarding incident handling efforts that referred to the virus by name.

Lastly, we found that the few federal components that either discovered or were alerted to the virus early did not effectively warn others. For example, Treasury told us that the U.S. Customs Service received an Air Force Computer Emergency Response Team (AFCERT) advisory early in the morning of May 4, but that Customs did not share this information with other Treasury bureaus.

Impact of the ILOVEYOU Outbreak on Federal Agencies

The lack of more effective early warning clearly affected most federal agencies. Only 7 of the 20 agencies we contacted were spared widespread infection, and this was largely because they relied on e-mail software other than Microsoft Outlook. Of the remaining agencies, the primary impact was e-mail disruption, which, in turn, slowed some agency operations and required agencies to divert technical staff toward stemming the virus' spread and cleaning "infected" computers. Of course, if an agency's business depends on e-mail for decision-making and service delivery, then the virus/worm probably had a significant impact on day-to-day operations in terms of lost productivity. While most agencies experienced disruptions of e-mail service for a day or less, eight agencies or agency components reported experiencing disruptions of longer than 1 day.

I would like to offer some highlights of our discussions with officials at individual agencies since they further complete the picture of the response efforts and damage resulting from ILOVEYOU.

- The Department of Health and Human Services (HHS) was inundated with about 3 million malicious messages. Departmental components experienced disruptions in e-mail service ranging from a few hours to as many as 6 days, and departmentwide e-mail communication capability was not fully restored until May 9. An HHS official observed that "if a biological outbreak had occurred simultaneously with this 'Love Bug' infestation, the health and stability of the Nation would have been compromised with the lack of computer network communication."

- At DOD, enormous efforts were expended containing and recovering from this virus. Military personnel from across the department were pulled from their primary responsibilities to assist. One DOD official noted that if such an attack were to occur over a substantial amount of time, reservists would have to be called for additional support. Some DOD machines required complete software reloads to overcome the extent of the damage.

- At least 1,000 files at NASA were damaged. While some files were recovered from backup media, others were not.

- At the Department of Labor, recovery required over 1,600 employee hours and over 1,200 contractor hours.
- The Social Security Administration required 5 days to become fully functional and completely remove the virus from its systems.
- The Department of Energy experienced a slowdown in external e-mail traffic, but suffered no disruption of mission-critical systems. Ten to 20 percent of DOE's machines nationwide required active cleanup.
- A vendor's 7:46 a.m. EDT warning to the Federal Emergency Management Agency enabled officials there to mitigate damage by restricting the packet size allowed through its firewalls until the necessary virus prevention software could be upgraded.
- As of May 10, the Veterans Health Administration (VHA) had received 7,000,000 "ILOVEYOU" messages, compared to a total of 750,000 received during the Melissa virus episode. VHA spent about 240 man hours to recover from the virus.
- The Department of Justice estimated spending 80 regular labor hours and 18 overtime hours for cleanup.
- Some of Treasury's components required manual distribution of updated virus signature files because automated means for rollout of software updates were not in place.
- The Department of Agriculture could not obtain the updated antivirus product it needed until after 1 p.m., in part because it had to compete with all of the vendor's other customers worldwide to obtain the updates.
- Effective user awareness programs were cited at the Department of Commerce, Treasury's Bureau of Public Debt, and the Department of Justice, where many infected messages were received but few were executed because users tended to be suspicious of unexpected and unusual e-mail messages and were not likely to open them.

Further Actions Required

Mr. Chairman, in many respects the federal government has been lucky. Even though ILOVEYOU and Melissa were disruptive, key government services remained largely operational through the events. However, the potential for more catastrophic damage is significant. Official estimates show that over 100 countries already have or are developing computer attack capabilities. Hostile nations or terrorists could use cyber-based tools and techniques to disrupt military operations, communications

networks, and other information systems or networks. The National Security Agency has acknowledged that potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems. According to Defense officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. According to a leading security software designer, viruses in particular are becoming more dangerous to computer users. In 1993 only about 10 percent of known viruses were considered destructive, harming files and hard drives. But now about 35 percent are regarded as harmful.

Such concerns highlight the need to improve the government's capacity and capability for responding to virus attacks. Clearly, more needs to be done to enhance the government's ability to collect, analyze, and distribute timely information that can be used by agencies to protect their critical information systems from possible attack. In the ILOVEYOU incident, NIPC and FedCIRC, despite their efforts, had only a limited impact on agencies being able to mitigate the attack.

At the same time, agencies can also take actions that would improve their ability to combat future virus attacks. For example, they can act to increase user awareness and understanding regarding unusual and suspicious e-mail and other computer-related activities. In particular, agencies can teach computer users that e-mail attachments are not always what they seem and that they should be careful when opening them. Users should never open attachments whose filenames end in ".exe" unless they are sure they know what they are doing. Users should also know that they should never start a personal computer with an unscanned floppy disk or CD-ROM in the computer drive.

Strengthening intrusion detection capabilities may also help. Clearly, it is difficult to sniff out a single virus attached to an e-mail coming in but if 100 e-mails with the same configuration suddenly arrive, an alert should be sounded. Furthermore, agencies can clarify policies and procedures for reporting and responding to unusual events and conduct "dry runs" on these procedures. They can ensure that up-to-date virus detection software has been installed on their systems. They can establish effective alternative communication mechanisms to be used when e-mail systems are not operating properly. And they can participate in interagency efforts to prepare for and share information on cyber threats, such as those sponsored by FedCIRC.

While such actions can go a long way toward helping agencies to ward off future viruses, they will not result in fully effective and lasting

improvements unless they are supported by strong security programs on the part of individual agencies and effective governmentwide mechanisms and requirements. As noted in previous testimonies and reports, almost every federal agency has poor computer security. Federal agencies are not only at risk from computer virus attacks, but are also at serious risk of having their key systems and information assets compromised or damaged from both computer hackers as well as unauthorized insiders.

We have recommended that agencies address these concerns by managing security risks on an entitywide basis through a cycle of risk management activities that include

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies to meet those needs,
- promoting awareness of policies and controls, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of these tools.

At the governmentwide level, this involves conducting routine periodic independent audits of agency security programs; developing more prescriptive guidance regarding the level of protection that is appropriate for their systems; and strengthening central leadership and coordination of information security related activities across government.

Mr. Chairman, this concludes my statement. The ILOVEYOU virus attack will not be our last incident. We hope it will provide an opportunity to examine our processes for developing threat assessments and providing warnings as well as an opportunity to examine our overall security posture.

We performed our review from May 8 through May 17, 2000, in accordance with generally accepted government auditing standards. For information about this testimony, please contact Jack L. Brock, Jr., at (202) 512-6240. Jean Boltz, Cristina Chaplain, Nancy DeFrancesco, Mike Gilmore, Danielle Hollomon, Paul Nicholas, and Alicia Sommers made key contributions to this testimony.

(511999)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)